GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

June 9, 2017

To: Subcommittee on Digital Commerce and Consumer Protection Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on "Disrupter Series: Update on IOT Opportunities and Challenges"

On **Tuesday, June 13, 2017, at 10:30 a.m. in room 2123 of the Rayburn House Office Building**, the Subcommittee on Digital Commerce and Consumer Protection will hold a hearing titled "Disrupter Series: Update on IoT Opportunities and Challenges." This hearing immediately follows an Internet of Things (IoT) Showcase in the Rayburn foyer, held from 9:00 a.m. to 11:00 a.m.

I. BACKGROUND

IoT generally refers to the ability of everyday objects to connect to the internet and to send and receive data.[1] IoT products are consumer products that use the internet as part of how they function, rather than devices used for accessing the internet such as computers, smartphones, or tables.[2]

[1] Federal Trade Commission, *Internet of Things: Privacy & Security in a Commercial World*, FTC Staff Report (Jan. 27, 2015).

[2] *Id.*

This subcommittee has held seven hearings on IoT topics as part of the Disrupter Series, including wearable devices, smart communities, health care apps, and a previous IoT hearing in 2015.[3] In 2016, Rep. Welch (D-VT) and Rep. Latta (R-OH) led a bipartisan IoT working group.[4]

II. CYBER SECURITY AND PRIVACY

Many IoT devices do not receive security updates or possess the capability to have vulnerabilities patched, leaving them particularly vulnerable to cyberattacks.[5] In October 2016, unsecured IoT devices were used to launch a distributed denial of service (DDoS) attack that took down some of the most frequented sites on the internet.[6] Yet, there are currently no federal requirements that mandate any level of security for IoT devices.[7]

Privacy concerns also have been raised because IoT devices function by collecting large amounts of data, which may also be shared with third parties.[8] The Federal Trade Commission (FTC) has broad authority to protect consumers from unfair or deceptive acts or practices, including poor privacy and security practices.[9] In 2015, the FTC released a staff report entitled, "Internet of Things: Privacy & Security in a Connected World," recommending that Congress enact baseline privacy legislation to increase consumer choice, require transparency, and mandate some level of privacy by design.[10]

III. WITNESSES

Cameron Javdani
Director of Sales and Marketing
Louroe Electronics

Bill Kuhns
President

---

[3] House Committee on Energy and Commerce, *Hearing on Internet of Things: Exploring the Next Technology Frontier,* 114th Cong. (Mar. 20, 2015).

[4] Rep. Peter Welch, *IoT Working Group Releases Report on Activities in the 114th Congress* (Jan. 4, 2017) (press release).

[5] House Committee on Energy and Commerce, Testimony of Bruce Schneier, Fellow, Berkman-Klein Center at Harvard University, *Hearing on Understanding the Role of Connected Devices in Recent Cyber Attacks*, 114th Cong. (Nov. 16, 2016).

[6] *Internet of Things' Hacking Attack Led to Widespread Outage of Popular Website*, NPR (Oct. 22, 2016).

[7] *Acting Federal Trade Commission Head: Internet of Things Should Self-Regulate*, The Guardian (Mar. 14, 2017).

[8] *See* note 1.

[9] 15 U.S.C. § 45(a).

[10] *See* note 1.

Vermont Energy Control Systems, LLC

William Marras, Ph.D.
Professor
Ohio State University Spine Research Institute

Peter Kosak,
Executive Director, Urban Active Solutions
General Motors North America

Mark Bachman, Ph.D.
CTO and Cofounder
Integra Devices

Gary Butler, Ph.D.
Founder, Chairman and CEO
Camgian Microsystems Corporation